UNITED STATES PATENT AND TRADEMARK OFFICE

50

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,913	05/11/2001	Sanguthevar Rajasekaran	20967000410	7607

20350 7590 06/10/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/853,913	RAJASEKARAN, SANGUTHEVAR	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-37 are pending.

2. Amendment filed 05/09/2005 has been received and considered.

Claim Rejections - 35 USC § 101

3. The rejection of claims 1-27 under 35 U.S.C. 101 have been withdrawn based on the amendments.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-9, 28-29, 33-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al ("Securing Threshold Cryptosystems against Chosen Ciphertext Attack") and further in view of Schneier ("Applied Cryptography").

As per claims 1, 28, 33, Shoup et al discloses, generating keys, encrypting a secret and distributing the secret to the owners at a custodian computer (see page 5).

Shoup et al fails to disclose the key generation and encryption technique being multiple-key public-key cryptography (in this case RSA), and deleting this information after distribution.

However, Schneier teaches the use of multiple-key public-key cryptography (RSA) and deletion of secrets (see page 527 where the K's are the d and $q_1 \ldots q_n$ and 184-185 for the deletion).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's multiple-key and deletion methods in the secret sharing of Shoup et al.

Motivation to do so would have been that RSA is the standard in much of the world (see page 474), and that old keys and old secrets must be deleted because they are valuable even if never used again (see page 184).

As per claims 2-4, the modified Shoup et al and Schneier system discloses receiving the n secret owner pieces (see Shoup et al page 5) and computing $S' = S^{dq} \bmod N$ for the first time and $S' = S'^{q} \bmod N$ for each time after that (see Schneier page 527 where d and $q_1 \ldots q_n$ are the $K_1 \ldots K_n$ and since in the applicants case

only one of the K's are sent per time it is known that Schneier's method can be done incremental rather than all at once as in the example).

As per claims 5, 29, 34, the modified Shoup et al and Schneier system discloses, at a custodian computer generating keys, encrypting a secret and distributing the secret to the owners (see Shoup et al page 5); the use of multiple-key public-key cryptography (RSA) for generating key's and encrypting the secret and deletion of secrets (see page 527 where the K's are the d and $q_1 \ldots q_n$ and 184-185 for the deletion).

As per claims 6-9, the modified Shoup et al and Schneier system discloses receiving the n secret owner pieces (see Shoup et al page 5) and computing $S' = S^{dq} \bmod N$ for the first time and $S' = S'^{q} \bmod N$ for each time after that and $S' = S'^{d'} \bmod N$ for the last instance (see Schneier page 527 where d, d' and $q_1 \ldots q_n$ are the $K_1 \ldots K_n$ and since in the applicants case only one of the K's are sent per time it is known that Schneier's method can be done incremental rather than all at once as in the example).

6. Claims 10-19, 30-31, 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Shoup et al and Schneier system and further in view of Graunke et al (U.S. 5,991,399).

As per claims 10, 30, 35, the modified Shoup et al and Schneier system discloses the choosing, computing of numbers for the multiple-key RSA at a custodian computer as described above (in this case the products of e, $e_1 \ldots e_n$, with d, $d_1 \ldots d_n$ are the K's), and distributing the secret pieces to the secret owners as above.

The modified Shoup et al and Schneier system fails to disclose generating and storing a database for the product of d and a unique number of the d_i's (part of the keys).

However, Graunke et al teaches storing a key in a database (see column 7 line 59 through column 8 line 9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Graunke et al's method of storing keys in a database to store the products of the modified Shoup et al and Schneier system.

Motivation to do so would have been to allow these products to be available to a server (see Graunke et al column 7 lines 59-66).

Claims 11-13 are rejected as in claims 2-4 above.

As per claim 14, in order to completely decrypt and restore the secret the correct value from the database must be accessed and used to compute the final exponential and modular operations).

As per claims 15-19, 31, 36, the modified Shoup et al, Schneier and Graunke et al system discloses computing $S^{ee'}$ (see Schneier page 527). Claims are 15-19, 31, 36 are rejected as in claims 10-15, 30, 35 above with the above mentioned addition.

7. Claims 20-24, 32, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al further in view of Schneier.

As per claim 20, 32, 37, Shoup et al discloses encrypting a secret, and performing a forward k out of n secret sharing algorithm by a custodian computer (see page 5).

Shoup et al fails to disclose deleting the secret.

However, Schneier teaches deleting a secret (see pages 184-185).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's deletion method in the secret sharing of Shoup et al.

Motivation to do so would have been that old keys and old secrets must be deleted because they are valuable even if never used again (see Schneier page 184).

As per claims 21-24, the modified Shoup et al and Schneier system discloses distributing the secrets, receiving the secrets, performing reverse k out of n secret sharing and decrypting to recreate the secret (see Shoup et al page 5).

8. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Shoup et al and Schneier system as applied to claim 20 above, and further in view of Shamir ("How to Share a Secret").

As per claim 25, the modified Shoup et al and Schneier system fails to disclose dividing the secret into k pieces and performing n polynomial evaluations at n points of a degree-k polynomial using the k pieces of the encrypted secret as polynomial coefficients; wherein each of the k secret owner pieces includes a result of one of the n polynomial evaluations and a corresponding one of the n points.

However, Shamir discloses such a break up (see page 613).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Shamir's method of polynomial break ups in the modified secret sharing method of Shoup et al and Schneier.

Motivation to do so would have been to create a k out of n threshold scheme (see Shamir page 612).

As per claims 26-27, the modified Shoup et al, Schneier and Shamir system discloses distributing the secret pieces and receiving k out of n of the pieces (see Shoup et al page 5), and performing reverse k out of n secret sharing by solving a system of generated linear equations (see Shamir page 613); assembling

and decrypting the pieces to recreate the secret (see Shoup et al page 5).

Response to Arguments

1. Applicant's arguments filed 05/09/2005 have been fully considered but they are not persuasive. Applicant argues: interpreting Shoup in view of Schneier would distribute K_i and N as opposed to S^d and q_i; the combination fails to disclose the method being performed by a custodian; Shoup teaches away from the given combination; claim 1 is not obvious over Schneier section 23.1 in view of section 23.2; there is no motivation to combine the references; the d' of claim 5 does not correspond to any of the K_i of Schneier; Schneier does give any motivation to combine the deleting of a secret with Shoup; the encryption step is not initially done before performing the secret sharing algorithm and there for it is not appropriate to combine the references; the e_id_i products do not correspond to the K_i of Schneier; Graunke does not disclose storing values that are a product of d and a unique k of the d_i numbers for $1 \leq i \leq n$ (ie the key retrieved from the database of Graunke does not depend on the user or users that sent the message, nor do the keys in Schneier).

Regarding Applicant's argument that interpreting Shoup in view of Schneier would distribute K_i and N as opposed to S^d and q_i, S^d is read as S^d mod N as described on page 11 lines 8-9, therefore as seen on page 527 $K_1,\ldots,K_{t-1}$ (where t-1 = n) (which are being distributed) would correspond to $q_1,\ldots,q_n$ and K_t would correspond to d. Therefore M^K mod n (which is the secret being distributed) would correspond to S^d mod N.

Regarding Applicant's argument that the combination fails to disclose the method being performed by a custodian, on Shoup page 5 the trusted dealer is the custodian.

Regarding Applicant's argument that Shoup teaches away from the given combination because the RSA method must be done in serial fashion, Shoup is merely relied upon for the teaching of generating keys, encrypting a secret and distributing the secret to the owners at a custodian computer and not the specifics of the method.

Regarding Applicant's argument that claim 1 is not obvious over Schneier section 23.1 in view of section 23.2, no rejection of Schneier section 23.1 in view of 23.2 has been made and therefore this argument is moot.

Regarding Applicant's argument that there is no motivation to combine the references, the motivation is as give above that

RSA is the standard encryption algorithm in much of the world as given from page 474 of Schneier.

Regarding Applicant's argument that the d' of claim 5 does not correspond to any of the K_i of Schneier because all the signers use all the keys, the bottom of Schneier page 527 is only an example of a use of the algorithm and when applied to Shoup not all the keys need to be used.

Regarding Applicant's argument that Schneier does give any motivation to combine the deleting of a secret with Shoup, as shown on page 184 of Schneier old secrets must be deleted because they are valuable even if never used again.

Regarding Applicant's argument that the encryption step is not initially done before performing the secret sharing algorithm and therefore it is not appropriate to combine the references, Shoup is merely relied upon for the teaching of generating keys, encrypting a secret and distributing the secret to the owners at a custodian computer and not the specifics of the method.

Regarding Applicant's argument that the $e_i d_i$ products do not correspond to the K_i of Schneier, a property of modular arithmetic is that if $a_1 \equiv 1 \bmod n$ and $b_1 \equiv 1 \bmod n$ then $a_1 b_1 \equiv 1 \bmod n$ (a printout from Wikipedia has been included as evidence

of this fact) so therefore the $e_i d_i$ products correspond to the K_i of Schneier.

Regarding Applicant's argument that Graunke does not disclose storing values that are a product of d and a unique k of the d_i numbers for $1 \leq i \leq n$ (ie the key retrieved from the database of Graunke does not depend on the user or users that sent the message, nor do the keys in Schneier), no where in claim 10 does is it reflected that a key is dependent on a user.

It is also noted that is the claims when n = 1 the system becomes general RSA as described on pages 466-474.

Conclusion

2. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Hardjono (US 6182214) teaches secret sharing.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER